Administering searchbases (continued)

searchbase_setlabel <searchbaseID> <searchbaselabel>

Specifies the label for a searchbase. This label is the name users will see. Users will not see the distinguished name specified by the searchbase_setdn command.

searchbase_userscansearch <searchbaseID> TRUE | FALSE

Specifies whether or not all users will be allowed to search for recipients in this searchbase (this argument has a value of either TRUE or FALSE). Set this command to "FALSE" in the rare circumstance when you don't want users to be able to encrypt files for other users in this searchbase.

Errors encountered when processing bulk command files

Results of processing bulk command files are saved to a .log file located in the directory you specified in the bulk console window. Errors appear in this form:

```
[<time-stamp>] <command-name>: ERROR
<context-specific-error-message>
```

where

- "time-stamp" is the time the command was executed in DD/MM/YYYY/HH:MM/SS format
- "command-name" is the name of the command executed
- "context-specific-error-message" is one or more lines of error message information specific to each instance of an unsuccessfully executed command

Additional documentation on Entrust/PKI 6.0 bulk commands

See "Administering multiple users" and "Bulk commands syntax summary" in *Using Entrust/PKI 6.0 on Windows* or *Using Entrust/PKI 6.0 on UNIX*.

Tcl syntax tips

Basic syntax: <command> <arg1> [<arg2>] …

\ used to:
- keep commands and arguments together if they span more than one line
- quote special characters
- turn off meaning of symbols such as "", { }, [ ], $

" " group words into single argument

{ } group words into single argument; elements such as [ ] and $ are not interpreted as Tcl syntax

Tcl resources

Practical Programming in Tcl and Tk Third Edition, Brent B. Welsh, Prentice Hall PTR
Graphical Applications with Tcl & Tk Second Edition, Eric Foster-Johnson, M&T Books
http://www.scriptics.com
http://www.beedub.com/book

Sample bulk scripts

Pre-authorizing a command, identifying a user, and issuing a command for a user

```
authorize user_updatekeypairs
user x "cn=Alice Gray + serialNumber=1QBB01, o=Your Company Inc, c=US"
user_updatekeypairs x
```

Adding users with customized properties

```
user y
user_settemplate y Person
user_setattribute y cn + "Alice Gray"
user_setattribute y sn + Gray
user_setattribute y serialNumber + 1YCAG01
user_addtodn y serialNumber
user_setattribute y mail + alice.gray@your_company.com
user_setparentdn y "o=Your Company Spinoff Inc, c=US"
user_setproperty y certificate_type Web web_default
user_setproperty y role "End User"
user_setproperty y group + "Group C"
user_setproperty y group + "Group G"
user_setproperty y key_expiry 30/03/2001 01/04/2001
user_setproperty y certificate_variable userStreet "100 East \
27th Street"
user_setproperty y certificate_variable userCity "New York"
user_setproperty y certificate_variable userEmail \
alice.gray@your_company.com
user_createdirentry y
user_add y
```

Changing a user's DN by creating new Directory entries

```
user x
user_settemplate x Person
user_setattribute x cn + "Alice Jones"
user_setattribute x sn + Jones
user_setattribute x serialNumber + AJYC123
user_setattribute x mail + alice.jones@your_company.com
user_setparentdn x "ou=Product Management,o=Your Company,c=US"
user_createdirentry x
user x "cn=Alice Gray,ou=Engineering,o=Your Company,c=US"
user_assigndn x "cn=Alice Jones,ou=Product Management,o=Your \
Company,c=US"
```

Changing a user's DN by renaming Directory entries

```
user y "cn=Alice Gray,ou=Engineering,o=Your Company,c=US"
user_setattribute y sn + Jones
user_setattribute y sn - Gray
user_renamedirentry y "cn=Alice Jones,ou=Product Management,\
o=Your Company,c=US"
user_assigndn y "cn=Alice Jones,ou=Product Management,o=Your \
Company,c=US"
```

Adding a searchbase

```
searchbase z Science "ou=Science,o=State University,c=US" TRUE
searchbase_add z
```

Creating a group

```
group x Sales
group_create x
```

Deleting a group

```
group x Sales
group_removeallusers x
group_delete x
```

Entrust/PKI bulk commands

Quick Reference

Release 6.0 for Windows and UNIX

How to use this card

< > indicate variables, for example, <command>

[ ] indicate options, for example, [newDN]

| indicates either/or parameters, for example, All | Latest

Pre-authorizing bulk commands

authorize <command>	Pre-authorizes a bulk command by collecting any additional authorizations required by the specified command.

Identifying a user

user <userID> [<userDN>] [New]	Identifies a user. The "userDN" option identifies a user by specifying the DN (distinguished name). "New" creates a new, customized Directory entry as opposed to a template-based user.
user_free <userID>	Frees the resources associated with a user object. Used when the user object associated with the userID is no longer required.

Adding users to Entrust/PKI

user_add <userID>	Adds a user to Entrust/Authority. User must already exist in the Directory. Also commits any user properties set with the user_setproperty command.
user_addtodn <userID> <attribute>	Specifies an additional attribute to include in the user's DN (distinguished name) when the user's Directory entry is created. Effective only when creating Directory entries using a template.
user_createdirentry <userID>	Creates an entry in the Directory with the Template method or the Custom method.
user_setparentdn <userID> <parentDN>	Specifies the DN (distinguished name) a new Directory entry is created under when the user_createdirentry command is issued for the userID. Effective only when creating a Directory entry using a template. The parent DN must already exist in the Directory. In the absence of this command, the user's Directory entry is created under the CA DN.
user_settemplate <userID> <template>	Sets the template for a new user entry. Only required when creating a new Directory entry using a template.

Setting up users for key recovery

user_cancelrecover <userID>	Returns a user to the Active state if they have been set for key recovery.
user_recover <userID>	Sets up a user for key recovery. User must be in the Active state.
user_reissueactivationcodes <userID>	Reissues a user's activation codes. User must be in the Added or Key Recovery state.

Deactivating and reactivating users

user_deactivate <userID>	Removes a user from Entrust. User must be in the Active, Key Recovery, or Added state.
user_reactivate <userID>	Adds a previously deactivated user to Entrust.

Revoking and deleting users

user_cancelhold <userID> <serialNumber> E | V Y | N	
	Cancels a hold put on a user's certificates.
<serialNumber>	The serial number of the certificate.
E | V	Indicates that the hold should be canceled on either the encryption (E) or verification (V) certificate.
Y | N	Indicates whether the CRL should be issued immediately: Y indicates that the CRL should be issued immediately, while N indicates that the CRL should not be issued immediately.
user_deletedirentry <userID>	Removes a user from the Directory.
user_revoke <userID> [<comment>] [<reason>] [All | Latest] [E | V | Both] \ [<last_uncompromised_date>]	
	Revokes a user's certificates, preventing the user from using them.
[<comment>]	Associates a comment with the revoked certificates. Default: No comment
[<reason>]	Specifies a reason for revocation. Valid reasons are: U (Unspecified), KC (Key Compromise), AC (Affiliation Change), S (Superseded), COO (Cessation Of Operation), or OH (On Hold). Default: Unspecified
[All | Latest]	Specifies whether to revoke all (including expired) certificates or only the most recent. Default: All
[E | V | Both]	Specifies which certificates to revoke: encryption (E), verification (V), or both (Both). Default: Both
[<last_uncompromised_date>]	Specifies the date the certificate(s) were last known to be uncompromised. Effective only if "reason" is "KC". Format is MM/DD/YYYY. If reason is "KC", default is issue date of the revoked certificate.

Changing user DNs (distinguished names)

user_assigndn <userID> <newDN>	Assigns a new DN to an Entrust user. The new DN must already exist in the Directory.
user_cancelchangedn <userID>	Cancels a change DN operation previously performed on an Entrust user. Works only if the user has not yet logged in and completed the change DN operation.
user_renamedirentry <userID> <newDN>	Renames a user's Directory entry. If the user is also an Entrust user, Entrust/Authority should also be updated using the user_assigndn command. Works only with LDAPv3-compliant Directories.

Changing user properties

user_applyproperties <userID>	Applies to the userID any user properties that have been modified using the user_setproperty command. Note: property modifications are not committed to Entrust/Authority until user_applyproperties is issued.
user_setproperty <userID> alternate_ID +|- [<value>]	
	Adds or deletes values from the alternate identity (also known as the e-mail or subjectAltName property). If the subtraction operator is used and no value is provided, the alternate identity is cleared.
user_setproperty <userID> certificate_type <category> <type>	
	Sets certificate category and type. When adding or importing a user into Entrust/Authority, the absence of this command implies the default certificate category (Enterprise) and type (ent_default) are to be used.

---

user_setproperty <userID> certificate_variable <variable> <value>	
	Assigns values to the certificate extension variables that are available for the user's certificate category and type. If the specified variable already has a value, the value will be replaced. The certificate category and type must be specified with user_setproperty ... certificate_type.
user_setproperty <userID> group +|- <groupname>	
	Sets group membership. A group must exist before adding users to it. Specifying group + * makes the user a member of all existing and future groups. Specifying group - * clears all group information. Users must belong to at least one group.
user_setproperty <userID> key_expiry [<PubEncKey_PrvSignKey_expiry> <PubVerKey_expiry>]	
	Sets key update options using key expiry. User must be set to key recovery with user_recover before setting key expiry dates. Date format depends on regional settings (for example, English [US] is MM/DD/YYYY). Date must be between 3 and 60 days from current date. PubVerKey_expiry must be later than PubEncKey_PrvSignKey_expiry. If set with no expiry arguments, the user will be set to the CA's default key update options. Overwrites the key_lifetimes property argument.
user_setproperty <userID> key_lifetimes [<PubEncKey_life> <PubVerKey_life> <PrvSignKey_life>]	
	Sets key update options using key lifetimes. PubEncKey_life and PubVerKey_life are in months (2-60). PrvSignKey_life is a percentage of PubVerKey_life (1-100). If set with no lifetime arguments, the user will be set to the CA's default key update options. Overwrites the key_expiry property argument.
user_setproperty <userID> role <roleID>	Sets a user's role. Valid roles are "End User", "Security Officer", "Administrator", "Directory Administrator", "Auditor", "AutoRA Administrator", and any custom roles created. Any roleID consisting of two or more words must be enclosed in quotation marks. A user can have only one role at a time.

Adding and deleting Directory attributes

user_setattribute <userID> <attribute> +|- [<value>]	
	Adds or deletes values from a user's Directory attribute. If the subtraction operator is used and "value" is an asterisk (*), the attribute and all its values are deleted.

Restoring user information to the Directory

user_restoretodir <userID>	Restores a user's Entrust-specific information to the Directory. The Directory entry for the userID must already exist.

Updating user key pairs

user_updatekeypairs <userID>	Updates a user's key pairs. The user's profile is updated with new keys the next time the user logs in. Cannot be canceled.

Archiving user key pair histories

user_archive <userID>	Writes an Entrust user's key history to a file on the machine hosting Entrust/Authority. All information on the user is cleared from the Entrust/Authority database.
user_retrieve <userID>	Retrieves a user's key history from the Entrust/Authority archive. User must already exist in the Directory as a non-Entrust user. Also commits any user properties that have been set with the user_setproperty command.

Exporting user key pair histories

user_export <userID> start <importCADN> [<newDN>]	
	Starts the operation to move a user from one CA to another. Writes a user's key history to file. This command is performed on the exporting CA. The importCADN argument identifies the DN (distinguished name) of the importing CA. If a newDN is not provided, it is assumed that the DN is unchanged. Puts the user in the Export Hold state.
user_export <userID> cancel	Cancels the user export operation. Moves the user from the Export Hold or Export state to the state they were in before the export operation. This command is performed on the exporting CA.
user_export <userID> finish	Completes the user export operation. Once the user has been imported into the importing CA, this command moves the user from the Export Hold to the Export state. This command is performed on the exporting CA.
user_import <userID> { <key_history_blob> }	
	Adds a user to Entrust and imports the user's encoded key history. This command is performed on the importing CA.

Administering groups

group <groupID> <groupname>	Identifies a group object.
group_create <groupID>	Creates a new group.
group_delete <groupID>	Deletes a group. Before deleting a group, remove all members from the group with group_removeallusers. As all members must belong to at least one group, one group must always exist.
group_removeallusers <groupID>	Removes all users from a group. You must remove all members from a group before deleting it. All users must belong to at least one group.

Administering searchbases

searchbase <searchbaseID> <searchbaseLabel> <searchbaseDN> <usersCanSearch>	
	Identifies a new searchbase.
<searchbaseLabel>	The label for the new searchbase that users will see.
<searchbaseDN>	The complete DN of the searchbase.
<usersCanSearch>	Specifies whether or not all users will be allowed to search for recipients in the new searchbase (this argument has a value of either TRUE or FALSE). Set this command to "FALSE" in the rare circumstance when you don't want users to be able to encrypt files for other users in the new searchbase.
searchbase_add <searchbaseID>	Adds a searchbase previously identified by the "searchbase" command. Note that before you add a searchbase with bulk commands, you must add an organizational unit in the Directory Browser.
searchbase_delete <searchbaseID>	Deletes a searchbase. When you delete a searchbase, the associated Directory entry is not automatically deleted. Users belonging to the searchbase are not deleted from the Directory. Rather, users' associations to the deleted searchbase are removed.
searchbase_setdn <searchbaseID> <searchbaseDN>	
	Specifies the DN of a searchbase. To include special characters such as commas or backslashes in a DN, escape the special characters using a backslash.